P-12

POLITICA DE CERTIFICACIÓN

CERTIFICADO DE PERSONA NATURAL

Última versión: **0.4**	Fecha de implementación: **06 de octubre de 2023**	
Preparado por: **DEPARTAMENTO DE CALIDAD Y ATENCIÓN AL USUARIO**  Firmado digitalmente por [F] NOMBRE RIVERA RAMOS JEAN AMILCAR - ID 8-804-1725 Fecha: 2023.10.04 08:19:31 -05'00'	**Revisado por:** **SUBCOMITÉ DE GESTIÓN DE POLÍTICAS** **ACTA DE SUBCOMITÉ DE GESTIÓN DE POLÍTICAS No. AR-2023-06**	**Aprobado por:** **COMITÉ EJECUTIVO** **ACTA DE COMITÉ EJECUTIVO No. AR-2023-07**

Índice

INTRODUCCIÓN

El presente documento corresponde a la Política de Certificación (PC) de los Certificados de Persona Natural emitidos por la Infraestructura de Clave Pública (en adelante PKI) del Registro Público de Panamá.

En esta PC se detalla y completa lo estipulado en la Declaración de Prácticas de Certificación (DPC) de la PKI del Registro Público de Panamá (en adelante, RPP-PKI), conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta Política de Certificación, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

La presente PC se ha estructurado teniendo en cuenta las recomendaciones de la (Request for comments) RFC 3647 “Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework”, de IETF. Con el propósito de facilitar la lectura y análisis del documento se incluyen todas las secciones establecidas en dicha RFC apareciendo la frase “No estipulado” en las secciones para las que no se haya previsto nada.

Todos los certificados que emite la PKI del Registro Público de Panamá son conformes con la versión 3 del estándar X.509, permitiendo la inclusión de extensiones para certificación de atributos.

1.1. Visión general

La PKI del Registro Público de Panamá (en adelante, RPP-PKI) se constituye como prestador de servicios de certificación de firma electrónica en virtud de la Ley Nº 82 de 2012, que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modificando la Ley Nº 51 de 2008 y adopta otras disposiciones. Nace con la finalidad de ofrecer los mecanismos y sistemas necesarios para garantizar la seguridad de las comunicaciones electrónicas en las que intervengan la Administración Pública, los profesionales y representantes de personas jurídicas que se relacionan con la Administración y los ciudadanos en general.

El presente documento es la norma básica del servicio de certificación, en la que se establecen su naturaleza, estructura y organización, así como los criterios y procedimientos que el Servicio se compromete a seguir en el ejercicio de su actividad, incluyendo desde la solicitud de los certificados y generación de las claves, hasta la posterior emisión, distribución, uso, revocación/suspensión y renovación de estos.

La presente Declaración de Prácticas de Certificación (en adelante DPC), emitida de conformidad con la Ley Nº 82 de 2012 y la Ley Nº 51 de 2008 define y fundamenta el marco normativo general, conforme al cual se desarrollará la actividad de Prestador del Servicio de Certificación de la República de Panamá, en relación con los procesos de solicitud, emisión y gestión del ciclo de vida de los certificados electrónicos, incluyendo los procedimientos de verificación de la vigencia, revocación y renovación de certificados.

Las Políticas de Certificación (en adelante PC) aplicables a cada clase de certificado complementan lo dispuesto con carácter general en la presente DPC. En caso de conflicto o contradicción entre lo

dispuesto en la Declaración de Prácticas de Certificación y las citadas Políticas, prevalecerá lo estipulado en estas últimas.

Las PC también definen el ámbito de potenciales titulares de los certificados, así como los usos previstos de los mismos y el conjunto de derechos y obligaciones que asumen el emisor, el titular de los certificados y los terceros que confían en los certificados emitidos por la RPP-PKI.

La actividad de RPP-PKI se desarrollará con plena sujeción a las prescripciones de la Ley Nº 82 de 2012 y la Ley Nº 51 de 2008.

Esta DPC asume que el lector conoce los conceptos de PKI, certificado y firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

1.2. Nombre del documento e identificación de la PC

Nombre del documento	Política de Certificación de Certificados de Persona Natural
Versión del documento	**0.4**
Estado del documento	Actualizado
Fecha de emisión	14/02/2014
Fecha de actualización	**22/09/2023** – Control de Cambios de Documentos No. 2023-22
Fecha de expiración	No aplicable
OID (Object Identifier)	2.16.591.1.2.2.1
Ubicación de la PC	https://www.firmaelectronica.gob.pa/politicas-certificacion.html

1.3. Participantes en la PKI

Las entidades y personas intervinientes en la PKI son las que se enumeran a continuación:

1. Prestador de Servicios de Certificación (PSC)
2. Autoridad de Aprobación de Políticas (AAP)
3. Autoridades de Certificación (CA)
4. Autoridades de Registro (RA)
5. Autoridades de Validación (VA)
6. Autoridades de Sellado de Tiempo (TSA)
7. Solicitantes y Titulares de certificados

8. Terceros que confían en los certificados de la PKI del Registro Público de Panamá

1.3.1. Prestador de Servicios de Certificación (PSC)

Según la definición dispuesta por la Ley Nº 51 de 2008 modificada por la Ley Nº 82 de 2012 un prestador de servicios de certificación es la persona jurídica que emite firmas electrónicas y los certificados electrónicos para identificar el propietario y el estatus de dichas firmas y provee otros servicios relacionados con el uso de las firmas electrónicas.

La Dirección Nacional de Firma Electrónica (en adelante DNFE) es un organismo dependiente del Registro Público de Panamá que actuará como prestador de servicios de certificación de la PKI del Registro Público de Panamá. La información legal y datos identificativos del Prestador de Servicios de Certificación estarán siempre disponibles en http://firmaelectronica.gob.pa/normativa/index.htm.

La DNFE desarrolla su actividad de conformidad con la legislación vigente en la materia, señalada en la Ley Nº 82 de 2012 y la Ley Nº 51 de 2008.

1.3.2. Autoridad de Aprobación de Políticas (AAP)

La Autoridad de Aprobación de Políticas (AAP) es la organización responsable de la aprobación de la DPC y de las Políticas de Certificación de la RPP-PKI, así como de la aprobación de las modificaciones de dichos documentos.

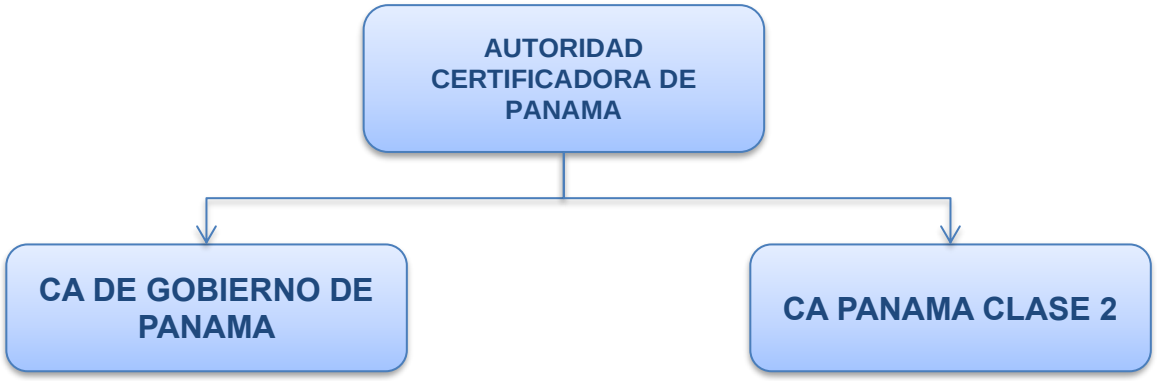
Asimismo, la AAP es la responsable, en caso de que se tuviese que evaluar la posibilidad de que una CA externa interactúe con la RPP-PKI, de determinar la adecuación de la DPC de dicha CA a la Política de Certificación afectada.

La AAP es responsable de analizar los informes de las auditorías, totales o parciales, que se hagan de la RPP-PKI, así como de determinar, en caso necesario, las acciones correctoras a ejecutar.

1.3.3. Autoridades de Certificación (CA)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la emisión de certificados electrónicos y de la asignación a sus titulares. Así mismo, efectúan la renovación y revocación de los mencionados certificados y la generación de claves públicas y privadas, cuando así lo establecen sus prácticas y políticas.

La arquitectura general, a nivel jerárquico, de la RPP-PKI es la siguiente:



1.3.3.1. Autoridad Certificadora de Panamá

La RPP-PKI emite todos los certificados objeto de esta PC bajo la jerarquía del Certificado Raíz. El certificado raíz es un certificado auto-firmado, en el que se inicia la cadena de confianza.

Subordinados al Certificado Raíz, se encuentran los certificados de jerarquía o de clave secundaria, que serán uno para los certificados de gobierno y otro para los certificados de clase 2.

El titular del certificado Raíz es el propio Registro Público de Panamá, y se emite y revoca por orden del Comité Ejecutivo.

Los datos más relevantes de la Autoridad Certificadora de Panamá son los siguientes:

Nombre distintivo	CN=AUTORIDAD CERTIFICADORA DE PANAMA, O=FIRMA ELECTRONICA, C=PA
Número de serie	403D B5E6 C915 73D4 518A 8515 6FE9 E7EC
Nombre distintivo del emisor	CN=AUTORIDAD CERTIFICADORA DE PANAMA, O=FIRMA ELECTRONICA, C=PA
Fecha de emisión	2013-05-08 12:02:13
Fecha de expiración	2053-05-08 12:02:13
Longitud de clave RSA	4096
Huella digital (SHA-1)	98BB 7426 2814 B7D9 FC41 3C2A 166C 1662 729E 24F8
URL de publicación del certificado	**http://www.pki.gob.pa/cacerts/caraiz.crt**
URL de publicación de la ARL	**http://www.pki.gob.pa/crls/caraiz.crl**

1.3.3.2. Autoridad de Certificación Panamá Clase 2

Bajo el Certificado Raíz de Panamá**,** se encuentran los certificados de **CA de Gobierno** y de **CA Panamá Clase 2**, bajo cuyas respectivas jerarquías se emiten a su vez todos los certificados que la DNFE emite a entidades finales.

Los Certificados de Profesional son emitidos por la **CA Panamá Clase 2**, cuyos datos más relevantes son los siguientes:

Nombre distintivo	CN=CA PANAMA CLASE 2, O=FIRMA ELECTRONICA, C=PA
Número de serie	71 84 c5 5b e9 40 a8 33 51 8c 0a 9e ff 29 15 97
Nombre distintivo del emisor	CN=AUTORIDAD CERTIFICADORA DE PANAMA, O=FIRMA ELECTRONICA, C=PA
Fecha de emisión	2013-05-09 15:44:14
Fecha de expiración	2033-05-09 15:44:14
Longitud de clave RSA	2048
Huella digital (SHA-1)	cf 79 f1 b8 4f 9f 22 80 d7 f3 da 21 1c c0 09 ef b4 e9 21 77
URL de publicación del certificado	**http://www.pki.gob.pa/cacerts/capc2.crt**
URL de publicación de la CRL	**http://www.pki.gob.pa/crls/capc2.crl**
Tipos de certificados emitidos	Autenticación de Persona Natural Firma de Persona Natural Autenticación de Representante de Persona Jurídica Firma de Representante de Persona Jurídica Autenticación de Colaborador de Persona Jurídica Firma de Colaborador de Persona Jurídica Autenticación de Profesional Firma de Profesional Autenticación de Factura Electrónica Firma de Factura Electrónica Servidor SSL Firma de Código

	Autenticación de Firma Electrónica Calificada en la Nube
	Firma de Firma Electrónica Calificada en la Nube
	Firma de Certificado de Sello de Empresa

1.3.4. Autoridades de Registro (RA)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la verificación de la identidad de los solicitantes de certificados electrónicos y, si procede, de los atributos asociados a los mismos.

Las Autoridades de Registro (RA) llevarán a cabo la identificación de los solicitantes de certificados conforme a las normas de esta PC y el acuerdo suscrito con la CA. Para ello, cada RA contará con un puesto de inscripción y un puesto de emisión:

1.3.4.1. Puesto de Inscripción

Las tareas realizadas en el puesto de inscripción son:

- Registro de datos de un solicitante de certificados electrónicos
- Verificación de la identidad de un solicitante de certificados electrónicos
- Personalización gráfica del dispositivo criptográfico en el que se generará el certificado electrónico que será entregado al solicitante.

1.3.4.2. Puesto de Emisión

Las tareas realizadas en el puesto de emisión son:

- Verificación de que el solicitante de certificados electrónicos ha realizado su registro en el puesto de inscripción
- Solicitud de los certificados a la CA correspondiente en función del perfil del certificado electrónico solicitado, así como su posterior entrega al titular.

1.3.5. Autoridades de Validación (VA)

La Autoridad de Validación (VA) tiene como función la comprobación del estado de los certificados emitidos por la RPP-PKI, mediante el protocolo *Online Certificate Status Protocol* (OCSP), que determina el estado actual de un certificado electrónico a solicitud de un tercero que confía sin requerir el acceso a listas de certificados revocados por éstas.

Este mecanismo de validación es complementario a la publicación de las listas de certificados revocados (CRL).

1.3.6. Autoridades de Sellado de Tiempo (TSA)

La Autoridad de Sellado de Tiempo (TSA) es la responsable de la prestación de los servicios recogidos a continuación, de forma que proporcione confianza a sus usuarios: solicitantes, titulares y terceros que confían.

Los servicios de sellado de tiempo se estructuran en dos partes:

- **Suministro de los sellos de tiempo**: los componentes técnicos y organizativos que emiten los sellos de tiempo (TST).
- **Gestión del sellado de tiempo**: los componentes técnicos y organizativos que supervisan y controlan la operativa del sellado de tiempo, incluyendo la sincronización temporal con la fuente de referencia UTC.

La TSA tiene la responsabilidad de operar una o varias Unidades de Sellado de Tiempo (TSU) las cuales crearán y firmarán los sellos de tiempo (TST) en nombre de la TSA. Cada TSU ha de tener su propia clave privada.

La TSA queda identificada en el certificado electrónico de firma que se utilice en el servicio de sellado de tiempo.

1.3.7. Solicitantes y titulares de certificados

Los solicitantes y titulares de certificados se encuentran definidos en la DPC de la RPP-PKI. Dentro del ámbito de la presente PC, los solicitantes y titulares de certificados de persona natural es cualquier persona natural que cuente con una cédula de identidad vigente o un extranjero residente en Panamá con un pasaporte vigente.

1.3.8. Terceros que confían en los certificados emitidos por la RPP-PKI

Los Terceros que confían son las personas o entidades diferentes del titular que deciden aceptar y confiar en los certificados emitidos por la CA Panamá Clase 2 con el fin de identificar un titular como persona natural.

1.4. Uso de los certificados

1.4.1. Usos adecuados de los certificados

Los certificados regulados por la presente PC sólo deben utilizarse con el propósito de autenticación o firma de personas naturales. Para determinar si es posible utilizar un certificado de persona natural para autenticación o firma es necesario comprobar el valor de la extensión ‘Key Usage’ del certificado en cuestión.

1.4.2. Limitaciones y restricciones en el uso de los certificados

Los certificados de persona natural no deben emplearse para ninguna actividad no especificada en el punto anterior.

1.5. Administración de las políticas

1.5.1. Entidad Responsable

Como establezca la DPC de la RPP-PKI.

1.5.2. Procedimiento de aprobación y modificación de la Política de Certificación de Certificados de Persona Natural

Como establezca la DPC de la RPP-PKI.

1.5.3. Datos de Contacto

Como establezca la DPC de la RPP-PKI.

1.6. Definiciones y Acrónimos

1.6.1. Definiciones

En el ámbito de la presente PC los términos empleados son los siguientes:

Autenticación: proceso de verificar la identidad de solicitante o titular de un certificado de la República de Panamá.

Certificado electrónico: documento electrónico expedido por un prestador de servicios de certificación de firmas electrónicas, que vincula los datos de verificación de una firma electrónica a un firmante y confirma su identidad.

Componente informático: cualquier dispositivo software o hardware susceptible de utilizar certificados electrónicos para su propio uso, con el objeto de identificarse o intercambiar datos firmados o cifrados con terceros aceptantes.

Identificación: proceso de establecer la identidad de un solicitante o titular de un certificado de la República de Panamá.

Infraestructura de Clave Pública: conjunto de individuos, políticas, procedimientos y sistemas de la información necesarios para proporcionar servicios de autenticación, cifrado, integridad y no repudio mediante el uso de criptografía de clave asimétrica y certificados electrónicos.

Prestador de Servicios de Certificación: persona jurídica que emite firmas electrónicas y los certificados electrónicos para identificar el propietario y el estatus de dichas firmas y provee otros servicios relacionados con el uso de las firmas electrónicas.

Solicitante: persona natural o jurídica que solicita un certificado electrónico para sí mismo o para un componente informático.

Titular: individuo o componente informático para el que se expide un certificado electrónico y es aceptado por éste o por su responsable en el caso de los certificados de componente.

Tercero que confía: persona o entidad diferente del titular, que decide aceptar y confiar en un certificado electrónico emitido por la DNFE.

1.6.2. Acrónimos

AAP: Autoridad de Aprobación de Políticas.

C: Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CA: Certification Authority (Autoridad de Certificación).

CDP: CRL Distribution Point (Punto de Distribución de CRL).

CN: Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CP: Certificate Policy (Política de Certificación).

CPS: Certification Practice Statement (Declaración de Prácticas de Certificación).

CRL: Certificate Revocation List (Lista de Revocación de Certificados).

CSR: Certificate Signing Request (petición de certificado). Conjunto de datos, que contienen una clave pública y su firma electrónica utilizando la clave privada asociada, enviado a la Autoridad de Certificación para la emisión de un certificado electrónico que contenga dicha clave pública.

CWA: CEN Workshop Agreement.

DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de un directorio X.500.

DNFE: Dirección Nacional de Firma Electrónica, del Registro Público de Panamá.

FIPS: Federal Information Processing Standard.

HSM: Hardware Security Module. Módulo de seguridad criptográfica empleado para el almacenamiento de claves y realización de operaciones criptográficas seguras.

IETF: Internet Engineering Task Force (Organismo de estandarización de Internet).

O: Organisation (Organización). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

OCSP: Online Certificate Status Protocol. Protocolo para la verificación online de la validez de un certificado electrónico.

OID: Object Identifier (Identificador Único de Objeto).

OU: Organisational Unit (Unidad Organizativa). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

PSC: Proveedor de Servicios de Certificación.

PIN: Personal Identificacion Number (Número de Identificación Personal). Password que protege el acceso a un dispositivo criptográfico.

PKCS: Public Key Cryptography Standards. Estándares de PKI desarrollados por los laboratorios de **RSA** aceptados internacionalmente.

RPP-PKI: Infraestructura de Clave Pública del Registro Público de Panamá.

PKI: Public Key Infrastructure (Infraestructura de Clave Pública).

PUK: PIN Unlock Key. Password que permite desbloquear un dispositivo criptográfico bloqueado por haber introducido en repetidas ocasiones un PIN erróneo de forma consecutiva.

RA: Registration Authority (Autoridad de Registro).

RFC: Request For Comments. Standard desarrollado por el IETF.

VA: Validation Authority (Autoridad de Validación).

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1. Repositorios

Como establezca la DPC de la RPP-PKI.

2.2. Publicación de información de certificación

Como establezca la DPC de la RPP-PKI.

2.3. Frecuencia de publicación

Como establezca la DPC de la RPP-PKI.

2.4. Controles de acceso a la información de certificación

Como establezca la DPC de la RPP-PKI.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Nombres

3.1.1. Tipos de nombres

Todos los titulares de certificados requieren un nombre distintivo (Distinguished Name) conforme con el estándar X.500.

A continuación, se define el procedimiento de asignación de los nombres distintivos para los certificados de persona natural de la RPP-PKI.

3.1.1.1. Certificado de autenticación

Campo	Valor	Descripción
C	PA	País
O	FIRMA ELECTRONICA	Organización
OU	PERSONA NATURAL	Unidad Organizacional
CN	[A] NOMBRE <apellidos nombre> – ID <cedula/pasaporte>	Nombre Común

3.1.1.2. Certificado de firma

Campo	Valor	Descripción
C	PA	País
O	FIRMA ELECTRONICA	Organización
OU	PERSONA NATURAL	Unidad Organizacional
CN	[F] NOMBRE <apellidos nombre> – ID <cedula/pasaporte>	Nombre Común

3.1.2. Necesidad de que los nombres sean significativos

En todos los casos los nombres distintivos de los titulares de los certificados deben ser significativos, ajustándose a las normas impuestas en el apartado anterior.

3.1.3. Reglas para interpretar varios formatos de nombres

La regla utilizada por RPP-PKI para interpretar los nombres distintivos de los titulares de certificados que emite es ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.4. Unicidad de los nombres

El conjunto de nombre distintivo (Distinguished Name) más el contenido de la extensión Policy Identifier debe ser único y no ambiguo. El uso del número de cédula de identidad o pasaporte en el CN garantiza la unicidad de este. De manera adicional, el prefijo [A] para el certificado de autenticación y el prefijo [F] para el de firma garantizan que el nombre distintivo sea distinto en cada caso.

3.1.5. Procedimientos de resolución de conflictos sobre nombres

Cualquier conflicto concerniente a la propiedad de nombres se resolverá según lo estipulado en el punto *9.13. Reclamaciones de esta PC*.

3.1.6. Reconocimiento, autenticación y papel de las marcas registradas

Como establezca la DPC de la RPP-PKI.

3.2. Validación inicial de la identidad

3.2.1. Medio de prueba de posesión de la clave privada

Las claves de los certificados de persona natural serán generadas por el titular de las mismas por lo que la posesión de la clave privada, correspondiente a la clave pública para la que solicita que se genere el certificado, quedará probada mediante el envío de la petición de certificado (CSR), en la cual se incluirá la clave pública firmada mediante la clave privada asociada.

3.2.2. Autenticación de la identidad de una persona jurídica

Este punto no es aplicable a esta PC. El procedimiento de autenticación de la identidad de una persona jurídica está documentado en la PC correspondiente.

3.2.3. Autenticación de la identidad de una persona natural

Para poder autenticar la identidad de la persona natural, el solicitante deberá comparecer en el puesto de inscripción con su cédula de identidad personal. Además, de los datos proporcionados en la solicitud, en el puesto de inscripción se capturarán los datos biométricos del solicitante.

3.2.4. Información no verificada sobre el solicitante

Toda la información recabada durante la expedición anterior ha de ser verificada.

3.2.5. Comprobación de las facultades de representación

Este punto no es aplicable ya que para poder autenticar la identidad de una persona natural este debe comparecer personalmente al puesto de inscripción con su cédula de identidad personal o pasaporte.

3.2.6. Criterios para operar con CA externas

Como establezca la DPC de la RPP-PKI.

3.3. Identificación y autenticación para solicitudes de renovación

La identificación y autenticación de los titulares de los certificados para las solicitudes de renovación por cualquier motivo especificado en el apartado 4.7 del presente documento se realizará mediante la cédula de identidad y el pasaporte de dicho titular.

3.4. Identificación y autenticación para solicitudes de revocación

La identificación y autenticación de los titulares de los certificados para las solicitudes de revocación por cualquier causa se realizará mediante la cédula de identidad o pasaporte de dicho titular.

4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. Solicitud de certificados

4.1.1. Quién puede efectuar una solicitud

La solicitud de certificado de persona natural será efectuada por la persona natural que vaya a ser titular del mismo.

4.1.2. Registro de las solicitudes de certificados y responsabilidades de los solicitantes

El procedimiento de solicitud de certificados de persona natural es el siguiente:

1. La persona natural que será titular del certificado electrónico realiza la preinscripción completando el formulario en la página web www.firmaelectronica.gob.pa.
2. En el formulario de prescripción deberá colocar su número de identificación o cédula (de ser panameño), que será validado automáticamente por el Sistema de Verificación de Identidad del Tribunal Electoral de Panamá (nombre, número de cédula, fecha de nacimiento); adicionalmente, debe colocar los datos adicionales, según el perfil del certificado electrónico solicitado, que para el caso de la presente política de certificación, será la dirección de correo electrónico.

   Para la validación de nacionales el operador de registro de la DNFE coteja la cédula de identidad personal contra el Sistema de Verificación de Identidad (SVI) del Tribunal Electoral.
3. De ser extranjero, en el formulario de preinscripción debe colocar el número de pasaporte, nombre completo, flecha de nacimiento, país de nacimiento y correo electrónico; Adicionalmente, debe adjuntar copia escaneada y legible del pasaporte y el certificado de estatus migratorio (extranjero residente) o el certificado de movimiento migratorio (extranjero no residente) emitido por el Servicio Nacional de Migración de Panamá.

   Para la validación, el operador de registro de la DNFE:

   - Coteja la información del solicitante contra el Sistema de Verificación de Identidad (SVI) del Tribunal Electoral si tiene carne de residente permanente o, a falta de dicho carné, coteja su pasaporte contra bases de datos en línea del Estado de la autoridad competente (Migración) o contra una certificación de estatus migratorio (extranjeros residentes) u certificación de movimiento migratorio (extranjeros no residentes) de esta entidad. La verificación del pasaporte contra certificaciones de Migración sólo se hará de no contar con el modo de verificación en línea.
4. Se conservará registrada, toda información y documentación relativa a la generación, suspensión y revocación de un certificado electrónico calificado, incluyendo la información suministrada por el suscriptor, así como las declaraciones de prácticas de certificación vigentes de cada momento, con un mínimo de siete (7) años contados desde el momento de la emisión del certificado electrónico de conformidad con el artículo 23 numeral 15 Ley 51 2008 modificada por la Ley 82 de 2012.

5. La documentación entregada por el solicitante queda almacenada en el CMS y puede ser consultada con el número de identificación de la persona natural solicitante o con el número de solicitud asignado por el CMS. La información y documentación entregada es sólo de carácter interno para propósito de validar la identidad del firmante y otros requeridos para la emisión del certificado electrónico, por lo que la DNFE se compromete a no utilizar esta información en otros aspectos que sean exclusivamente relacionados con sus actividades como prestador de servicios de certificación.

   En el caso que una solicitud haya sido realizada incorrectamente por el solicitante, este deberá solicitar a la DNFE, vía telefónica o por correo electrónico, la eliminación de la solicitud, en este caso, tanto la información, como la documentación aportada serán eliminada del CMS.

6. El día de la cita, el solicitante se presenta a la DNFE y se identifica con su cédula de identidad personal.

7. En el puesto de inscripción se realizará el registro de los datos biométricos del solicitante, así como la expedición de su dispositivo criptográfico. Para proceder a la expedición del dispositivo criptográfico, es necesario que éste haya firmado el documento de licencia de uso y aceptación de condiciones.

8. Una vez que el solicitante haya firmado el documento de licencia de uso y aceptación de condiciones, en el puesto de emisión se procederá a la generación de sus certificados en el dispositivo criptográfico que acaba de obtener el solicitante.

Es responsabilidad del solicitante garantizar la completitud y veracidad de toda la información aportada para obtener sus certificados de persona natural con independencia de las comprobaciones realizadas por el prestador de servicios de certificación para verificarla.

4.2. Tramitación de las solicitudes de certificados

4.2.1. Realización de las funciones de identificación y autenticación

La realización de las funciones de identificación y autenticación requerirá la presencia física del solicitante junto con su cédula de identificación personal en el puesto de inscripción. En el puesto de emisión, la identificación y autenticación del usuario se realizará con el dispositivo criptográfico que éste ha obtenido en el puesto de inscripción.

El proceso de identificación y autenticación de un solicitante está descrito en el apartado 3.2.3 del presente documento.

4.2.2. Aprobación o denegación de las solicitudes de certificados

La emisión del certificado tendrá lugar una vez que la RPP-PKI haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación. El procedimiento por el que se determina la naturaleza y la forma de realizar dichas comprobaciones se establece en el apartado anterior.

RPP-PKI puede negarse a emitir un certificado de cualquier solicitante basándose exclusivamente en su propio criterio, sin que ello implique contraer responsabilidad alguna por las consecuencias que pudieran derivarse de tal negativa.

4.2.3. Plazo para la tramitación de las solicitudes de certificados

Las CA de la RPP-PKI no se hacen responsables de las demoras que puedan surgir en el período comprendido entre la solicitud del certificado y la entrega de este. En cualquier caso, el plazo para la tramitación de las solicitudes de certificados vendrá limitado por la disponibilidad de citas en los puestos de inscripción y emisión a los que desee acudir el solicitante.

4.3. Emisión de certificados

4.3.1. Actuaciones de la CA durante la emisión del certificado

La emisión del certificado implica la autorización definitiva de la solicitud por parte de la CA. Cuando alguna de las CA de la RPP-PKI emita un certificado de acuerdo con una solicitud de certificación efectuará las notificaciones que se establecen en el apartado 4.3.2. del presente capítulo.

Todos los certificados iniciarán su vigencia en el momento de su emisión y será de dos años, contados a partir de la fecha y hora de su emisión y concluye cuando haya pasado el tiempo de vigencia que se encuentra en el propio certificado electrónico.

El periodo de vigencia podrá estar sujeto a una posible extinción anticipada, temporal o definitiva, cuando se den las causas que motiven la suspensión o revocación del certificado.

4.3.2. Notificación al solicitante de la emisión por la CA del certificado

La emisión del certificado electrónico de Persona Natural es presencial por lo tanto la notificación es inmediata. En el momento de la entrega de la cédula de identidad personal y la copia del documento de aceptación de condiciones firmado se le indica al suscriptor su responsabilidad en el uso de su certificado electrónico. De igual forma se le indicará como obtener la presente PC.

4.4. Aceptación del certificado

4.4.1. Mecanismo de aceptación del certificado

El titular del certificado electrónico de persona natural da acceso a la tarjeta criptográfica mediante el PIN aceptando la generación de su certificado.

4.4.2. Publicación del certificado por la CA

Este punto no es aplicable ya que los certificados electrónicos de Persona Natural no se publicarán en ningún repositorio.

4.4.3. Notificación de la emisión del certificado por la CA a otras Autoridades

Cuando alguna de las CA de la RPP-PKI emita un certificado de acuerdo con una solicitud de certificación tramitada a través de una RA, enviará una copia de este a la RA que remitió la solicitud.

4.5. Par de claves y uso del certificado

Los Certificados de Persona Natural son certificados de uso intransferible que acreditan la identidad de su titular.

4.5.1. Uso de la clave privada y del certificado por el titular

El titular sólo podrá utilizar la clave privada y el certificado para los usos autorizados en esta PC y de acuerdo con lo establecido en los campos 'Key Usage' y 'Extended Key Usage' del certificado. Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso, establecidas en la DPC y PC, y sólo para la realización de funciones que requieran acreditar la identidad del titular como persona natural.

Tras la expiración o revocación del certificado el titular dejará de usar la clave privada.

4.5.2. Uso de la clave pública y del certificado por los terceros aceptantes

Los Terceros que Confían sólo pueden depositar su confianza en los certificados para la realización de funciones que requieran acreditar la identidad del titular como persona natural y de acuerdo con lo establecido en el campo 'Key Usage' y 'Extended Key Usage' del certificado.

Los Terceros que Confían han de realizar las operaciones de clave pública de manera adecuada para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los mecanismos establecidos en la DPC de la RPP-PKI y en la presente PC.

Asimismo, se adhieren a las condiciones de uso establecidas en dichos documentos.

4.6. Renovación de certificados sin cambio de claves

4.6.1. Circunstancias para la renovación de certificados sin cambio de claves

Todas las renovaciones de certificados realizadas en el ámbito de esta PC se realizarán con cambio de claves. En consecuencia, no se recogen el resto de los puntos referente a renovación de certificados sin cambio de claves (puntos 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7) que establece la RFC 3647, lo que implica, a efectos de esta DPC, su no estipulación.

4.6.2. Quién puede solicitar la renovación de los certificados sin cambio de claves

No estipulado.

4.6.3. Tramitación de las peticiones de renovación de certificados sin cambio de claves

No estipulado.

4.6.4. Notificación de la emisión de un nuevo certificado al titular

No estipulado.

4.6.5. Forma de aceptación del certificado sin cambio de claves

No estipulado.

4.6.6. Publicación del certificado sin cambio de claves por la CA

No estipulado.

4.6.7. Notificación de la emisión del certificado por la CA a otras Autoridades

No estipulado.

4.7. Renovación de certificados con cambio de claves

4.7.1. Circunstancias para una renovación con cambio claves de un certificado

Todas las renovaciones de certificados de la RPP-PKI se realizarán con cambio de claves.

Algunos de los motivos, entre otros, por los que se puede renovar un certificado con cambio de claves son:

- Expiración del periodo de validez
- Tarjeta criptográfica deteriorada.
- Cambio de datos contenidos en el certificado.
- Claves comprometidas o pérdida de fiabilidad de estas.
- Cambio de formato.

Previo a la fecha de caducidad del certificado, el suscriptor recibirá de la DNFE una notificación de recordatorio del vencimiento, que será enviada a la dirección de correo electrónico suministrada durante la emisión del certificado, sin embargo, no es obligación de la DNFE garantizar la efectividad de la notificación sobre la terminación de la vigencia de su certificado electrónico o confirmar la recepción de la misma, pues es una obligación del suscriptor, conocer la vigencia de su certificado electrónico y adelantar los trámites pertinentes ante la DNFE para la emisión de su nueva firma electrónica.

La renovación se entenderá como la emisión de un nuevo certificado electrónico, por lo que, implica el registro de una nueva solicitud que estará sujeta a la validación de la identidad por parte de la RA y la generación de un nuevo par de claves.

4.7.2. Quién puede solicitar la renovación de los certificados

La renovación de los certificados únicamente debe ser solicitada por el titular, cuando se encuentre próximo a vencer el certificado y cuando desee continuar utilizándolo; adicionalmente, podrá solicitarlo si se cumplen algunos de los motivos especificados en el apartado 4.7.1 del presente documento.

4.7.3. Tramitación de las peticiones de renovación de certificados con cambio de claves

La RA comprobará en el proceso de renovación que la información utilizada para verificar la identidad y atributos del titular es todavía válida. Si alguna información del titular ha cambiado ésta deberá ser verificada y registrada con el acuerdo del titular.

La solicitud de renovación de certificados con cambio de claves se realizará de forma presencial en el puesto de emisión. Para la identificación y autenticación del usuario éste deberá presentar su cédula de identidad o pasaporte y, a no ser que se haya perdido por cualquier causa el dispositivo criptográfico donde se emitieron los certificados a renovar deberá presentarse dicho dispositivo criptográfico.

En cualquier caso, la renovación de un certificado está supeditada a:

- Que se solicite en debido tiempo y forma, siguiendo las instrucciones y normas que RPP-PKI específica a tal efecto.
- Que la CA no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación / suspensión del certificado.
- Que la solicitud de renovación de los servicios de prestación se refiera al mismo tipo de certificado emitido inicialmente.

4.7.4. Notificación de la emisión de un nuevo certificado al titular

La emisión del nuevo certificado electrónico a Persona Natural es presencial por lo tanto la notificación es inmediata mediante la comunicación de la finalización satisfactoria del proceso de renovación del certificado electrónico.

4.7.5. Forma de aceptación del certificado con las claves cambiadas

El solicitante deberá volver a firmar el documento de aceptación de condiciones para poder proceder a la renovación del certificado con cambio de claves.

4.7.6. Publicación del certificado con las nuevas claves por la CA

Este punto no es aplicable ya que la RPP-PKI, una vez emitido el certificado, no los publica en repositorios.

4.7.7. Notificación de la emisión del certificado por la CA a otras Autoridades

Cuando la CA de la RPP-PKI emita un certificado de acuerdo con una solicitud de certificación tramitada a través de una RA, enviará una copia de este a la RA que remitió la solicitud.

4.8. Modificación de certificados

4.8.1. Circunstancias para la modificación de un certificado

Durante el ciclo de vida de un certificado electrónico, no se tiene prevista la modificación/actualización de los campos contenidos en dicho certificado. Si se requiere un cambio en los datos del certificado emitido, será necesario revocar el certificado y emitir uno nuevo con las modificaciones correspondientes.

Las modificaciones de los certificados pueden provenir de diferentes motivos tales como:

- Cambio de nombre.
- Reorganización como resultado del cambio en el nombre distintivo (DN).

Todas las modificaciones de certificados realizadas en el ámbito de esta PC se tratarán como una renovación de certificados, por lo que son de aplicación los apartados anteriores al respecto.

4.8.2. Quién puede solicitar la modificación de los certificados

Este punto no es aplicable ya que los casos de modificaciones del certificado electrónico a persona natural serán tratados como una renovación de certificados, por lo que le aplican los apartados anteriores al respecto. En consecuencia, no se recogen el resto de los puntos referente a modificación de certificados (puntos 4.8.3, 4.8.4, 4.8.5, 4.8.6, 4.8.7) que establece la RFC 3647, lo que implica, a efectos de esta DPC, su no estipulación.

4.8.3. Tramitación de las peticiones de modificación de certificados

No estipulado.

4.8.4. Notificación de la emisión de un certificado modificado al titular

No estipulado.

4.8.5. Forma de aceptación del certificado modificado

No estipulado.

4.8.6. Publicación del certificado modificado por la CA

No estipulado.

4.8.7. Notificación de la modificación del certificado por la CA a otras Autoridades

No estipulado.

4.9. Revocación y suspensión de certificados

4.9.1. Circunstancias para la revocación

La revocación de un certificado es el acto por el cual se inhabilita un certificado electrónico antes de su caducidad. El efecto de la revocación de un certificado es el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación. La revocación de un certificado impide el uso legítimo del mismo por parte del titular.

La revocación de un certificado implica su publicación en la Lista de Certificados Revocados (CRL) de acceso público. Al expirar el periodo de validez de un Certificado revocado, éste dejará de estar incluido en la CRL.

Sin perjuicio de lo dispuesto en la normativa aplicable un certificado podrá ser revocado por:

- El robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del titular.
- El mal uso deliberado de claves y certificados, o la falta de observancia o contravención de los requerimientos operacionales contenidos en el Formulario de aceptación de las condiciones de los servicios de certificación de la autoridad de certificación de la RPP-PKI, la PC asociada o de la presente DPC.
- El titular de un certificado deja de pertenecer al grupo, circunstancia que le facultaba para la posesión del certificado.
- El cese de la actividad de la RPP-PKI.
- Emisión defectuosa de un certificado debido a que:
    - No se ha cumplido un requisito material para la emisión del certificado.
    - La creencia razonable de que un dato fundamental relativo al certificado es o puede ser falso.
    - Existencia de un error de entrada de datos u otro error de proceso.
- El par de claves generado por un titular se revela como “débil”.
- La información contenida en un certificado o utilizada para realizar su solicitud deja de ser correcta.
- Por orden formulada por el titular o por tercero autorizado.
- El certificado de una RA o CA superior en la jerarquía de confianza del certificado es revocado.
- Por la concurrencia de cualquier otra causa especificada en la DPC o en la presente PC.

La revocación tiene como principal efecto sobre el certificado la terminación inmediata y anticipada del periodo de validez de este, deviniendo el certificado como no válido. La revocación no afectará a las obligaciones subyacentes creadas o comunicadas por esta PC ni tendrá efectos retroactivos.

4.9.2. Quién puede solicitar la revocación

El suscriptor podrá voluntariamente, el cualquier momento, de manera directa, solicitar a la DNFE la revocación de su certificado electrónico emitido, en cuyo caso se iniciará el procedimiento de revocación del certificado electrónico.

La RPP-PKI o cualquiera de las Autoridades que la componen podrá tramitar la revocación de un certificado si tuviera conocimiento o sospecha del compromiso de la clave privada del suscriptor o cualquier otro hecho determinante que requiera revocar el certificado.

4.9.3. Procedimiento de solicitud de revocación

La solicitud de revocación del certificado la debe efectuar el titular del certificado electrónico, de la siguiente manera:

1. A través de correo electrónico a servicios@firmaelectrónica.gob.pa.pa, adjuntando una nota formal de solicitud y firmado con su firma electrónica u hológrafa, esta última debe coincidir con su firma registrada en su documento de identidad personal o de manera presencial, en las instalaciones de la DNFE de lunes a viernes en el horario de 8:00 am a 04:00 pm (días hábiles), entregando una nota de solicitud formal y presentando su documento de identidad personal.
2. El operador de registro realiza la verificación correspondiente de los datos suministrados en la nota de solicitud realiza la revocación en caso de conformidad.
3. El operador de registro envía un correo al suscriptor del certificado informando sobre la revocación del certificado electrónico.

La solicitud de revocación también la puede realizar La RPP-PKI o cualquiera de las Autoridades que la componen pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del titular o cualquier otro hecho determinante que recomendara emprender dicha acción.

4.9.4. Periodo de gracia de la solicitud de revocación

La revocación se llevará a cabo de forma inmediata a la tramitación de cada solicitud verificada como válida. Por tanto, no existe ningún periodo de gracia asociado a este proceso durante el que se pueda anular la solicitud de revocación.

4.9.5. Plazo en el que la CA debe resolver la solicitud de revocación

Las solicitudes de revocación deben resolverse tan rápido como sea posible en un tiempo no superior a 24 horas en días laborables y nunca superior a 72 horas en fines de semana y/o días festivos.

4.9.6. Requisitos de verificación de las revocaciones por los terceros que confían

Como establezca la DPC de la RPP-PKI.

4.9.7. Frecuencia de emisión de CRL

Como establezca la DPC de la RPP-PKI.

4.9.8. Tiempo máximo entre la generación y la publicación de las CRL

El tiempo máximo entre la generación de una CRL y su correspondiente publicación en el repositorio es de 6 horas.

4.9.9. Disponibilidad de un sistema en línea de verificación del estado de los certificados

Como establezca la DPC de la RPP-PKI.

4.9.10. Requisitos de comprobación en línea de revocación

Como establezca la DPC de la RPP-PKI.

4.9.11. Otras formas de divulgación de información de revocación disponibles

No estipulado.

4.9.12. Requisitos especiales de revocación de claves comprometidas

No hay ninguna variación en las cláusulas anteriores cuando la revocación sea debida al compromiso de la clave privada.

4.9.13. Causas para la suspensión

La suspensión de la vigencia de los certificados se aplicará, entre otros, en los siguientes casos:

- Cambio temporal de alguna de las circunstancias del titular del certificado que aconsejen la suspensión de los certificados mientras dure el mismo. Al retornarse a la situación inicial se levantará la suspensión del certificado.
- Comunicación por el titular del certificado de un posible compromiso de sus claves. En el caso de que la sospecha, por su grado de certeza, no aconseje la revocación inmediata, se suspenderán los certificados del titular mientras se averigua el posible compromiso de las claves. Al término del análisis se determinará si se revocan los certificados o si se levanta la suspensión.

4.9.14. Quién puede solicitar la suspensión

La solicitud debe presentarla el titular del certificado.

4.9.15. Procedimiento para la solicitud de suspensión

En caso de pérdida o deterioro de su dispositivo criptográfico, un titular de certificados de persona natural podrá solicitar la suspensión temporal de los mismos vía telefónica al número **+507 504 3900** o correo electrónico a la dirección **servicios@firmaelectronica.gob.pa** En este caso, el usuario deberá dar su número de cédula y sus códigos de suspensión para identificarse.

Adicional, la suspensión podrá solicitarse mediante el mismo procedimiento establecido para la revocación en el apartado 4.9.3 del presente documento.

El operador de registro realiza la verificación correspondiente de los datos suministrados en la nota de solicitud o la información proporcionada por el suscriptor, donde el código de suspensión debe coincidir con el registrado en el sistema y realiza la suspensión en caso de conformidad.

El operador de registro envía un correo al suscriptor del certificado informando sobre la suspensión del certificado electrónico

Una vez realizada la suspensión del certificado electrónico, una entrada para el certificado suspendido permanece en la CRL sin más acción.

Si posteriormente, el titular de los certificados electrónicos solicita la revocación (según lo indicado en el apartado 4.9.3) de un certificado suspendido la entrada de CRL para el certificado suspendido se reemplaza por una entrada de revocación para el mismo certificado.

Si el titular de los certificados electrónicos solicita la activación de un certificado suspendido, el certificado suspendido se libera explícitamente y la entrada se elimina de la CRL.

4.9.16. Límites del periodo de suspensión

No se establece un plazo máximo de suspensión de la vigencia de los certificados.

Si durante el tiempo de suspensión del certificado éste caduca o se solicita su revocación, se producirán las mismas consecuencias que para los certificados no suspendidos en esos mismos casos de caducidad o revocación.

4.10. Servicios de información del estado de certificados

4.10.1. Características operativas

Como establezca la DPC de la RPP-PKI.

4.10.2. Disponibilidad del servicio

Como establezca la DPC de la RPP-PKI.

4.10.3. Características adicionales

Como establezca la DPC de la RPP-PKI.

4.11. Extinción de la validez de un certificado

Como establezca la DPC de la RPP-PKI.

4.12. Custodia y recuperación de claves

4.12.1. Prácticas y políticas de custodia y recuperación de claves

Este punto no es aplicable ya que los datos de creación de certificado electrónico de persona natural (clave privada) se generan dentro de una tarjeta criptográfica y no pueden ser exportadas en ningún caso. La responsabilidad de la custodia de la tarjeta criptográfica donde está contenido el certificado electrónico recae enteramente sobre el titular.

4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión

Este punto no aplica ya que la recuperación de la clave de sesión es responsabilidad del suscriptor del certificado electrónico; el método de recuperación empleado es a través de un número PUK que se le entrega al suscriptor al momento de generarse su tarjeta criptográfica.

5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

5.1. Controles físicos

5.1.1. Ubicación física y construcción

Como establezca la DPC de la RPP-PKI.

5.1.2. Acceso físico

Como establezca la DPC de la RPP-PKI.

5.1.3. Alimentación eléctrica y aire acondicionado

Como establezca la DPC de la RPP-PKI.

5.1.4. Exposición al agua

Como establezca la DPC de la RPP-PKI.

5.1.5. Prevención y protección frente a incendios

Como establezca la DPC de la RPP-PKI.

5.1.6. Sistema de almacenamiento

Como establezca la DPC de la RPP-PKI.

5.1.7. Eliminación de residuos

Como establezca la DPC de la RPP-PKI.

5.1.8. Copias de seguridad fuera de las instalaciones

Como establezca la DPC de la RPP-PKI.

5.2. Controles de procedimiento

5.2.1. Roles responsables del control y gestión de la PKI

Como establezca la DPC de la RPP-PKI.

5.2.2. Número de personas requeridas por tarea

Como establezca la DPC de la RPP-PKI.

5.2.3. Roles que requieren segregación de funciones

Como establezca la DPC de la RPP-PKI.

5.3. Controles de personal

5.3.1. Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

Como establezca la DPC de la RPP-PKI.

5.3.2. Procedimientos de comprobación de antecedentes

Como establezca la DPC de la RPP-PKI.

5.3.3. Requerimientos de formación

Como establezca la DPC de la RPP-PKI.

5.3.4. Requerimientos y frecuencia de actualización de la formación

Como establezca la DPC de la RPP-PKI.

5.3.5. Frecuencia y secuencia de rotación de tareas

Como establezca la DPC de la RPP-PKI.

5.3.6. Sanciones por actuaciones no autorizadas

Como establezca la DPC de la RPP-PKI.

5.3.7. Requisitos de contratación de terceros

Como establezca la DPC de la RPP-PKI.

5.3.8. Documentación proporcionada al personal

Como establezca la DPC de la RPP-PKI.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

Como establezca la DPC de la RPP-PKI.

5.4.2. Frecuencia de procesado de registros de auditoría

Como establezca la DPC de la RPP-PKI.

5.4.3. Periodo de conservación de los registros de auditoría

Como establezca la DPC de la RPP-PKI.

5.4.4. Protección de los registros de auditoría

Como establezca la DPC de la RPP-PKI.

5.4.5. Procedimientos de respaldo de los registros de auditoría

Como establezca la DPC de la RPP-PKI.

5.4.6. Sistema de recogida de información de auditoría (interno vs externo)

Como establezca la DPC de la RPP-PKI.

5.4.7. Notificación al sujeto causa del evento

Como establezca la DPC de la RPP-PKI.

5.4.8. Análisis de vulnerabilidades

Como establezca la DPC de la RPP-PKI.

5.5. Archivado de registros

5.5.1. Tipo de eventos archivados

Como establezca la DPC de la RPP-PKI.

5.5.2. Periodo de conservación de registros

Como establezca la DPC de la RPP-PKI.

5.5.3. Protección del archivo

Como establezca la DPC de la RPP-PKI.

5.5.4. Procedimientos de copia de respaldo del archivo

Como establezca la DPC de la RPP-PKI.

5.5.5. Requerimientos para el sellado de tiempo de los registros

Como establezca la DPC de la RPP-PKI.

5.5.6. Sistema de archivo de información de auditoría (interno vs externo)

Como establezca la DPC de la RPP-PKI.

5.5.7. Procedimientos para obtener y verificar información archivada

Como establezca la DPC de la RPP-PKI.

5.6. Cambio de claves

Como establezca la DPC de la RPP-PKI.

5.7. Recuperación ante compromiso de clave o catástrofe

5.7.1. Procedimientos de gestión de incidentes y compromisos

Como establezca la DPC de la RPP-PKI.

5.7.2. Alteración de los recursos hardware, software y/o datos

Como establezca la DPC de la RPP-PKI.

5.7.3. Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad

Como establezca la DPC de la RPP-PKI.

5.7.4. Instalación después de un desastre natural u otro tipo de catástrofe

Como establezca la DPC de la RPP-PKI.

5.8. Cese de una CA o RA

5.8.1. Autoridad de Certificación

Como establezca la DPC de la RPP-PKI.

5.8.2. Autoridad de Registro

Como establezca la DPC de la RPP-PKI.

6. CONTROLES DE SEGURIDAD TÉCNICA

Los controles de seguridad técnica aplicables a los diferentes componentes de la PKI se encuentran descritos en la DPC de la RPP-PKI. En este apartado únicamente se describen los controles de seguridad técnica particulares del tipo de certificados tratado.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

Los pares de claves para los certificados de persona natural se generan en dispositivos criptográficos hardware con certificación FIPS 140-2 Nivel 2.

6.1.2. Entrega de la clave privada al titular

La clave privada de los certificados de persona natural es generada por el propio titular en su dispositivo criptográfico, por lo que en ningún caso será entregada al mismo.

6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública de los certificados de persona natural se genera en el dispositivo criptográfico del titular en el puesto de emisión siendo la RA la responsable de entregar dicha clave pública a la CA.

6.1.4. Entrega de la clave pública de la CA a los terceros que confían

La clave pública de las CA de la RPP-PKI está a disposición de los terceros que confían en el Repositorio de la RPP-PKI (ver apartado 2.1).

6.1.5. Tamaño de las claves

El tamaño de las claves de los certificados de persona natural es de 2048 bits.

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

La clave pública de los certificados de persona natural de la RPP-PKI está codificada de acuerdo con RFC 3280 y PKCS#1 siendo el algoritmo de generación de claves RSA.

6.1.7. Usos admitidos de la clave (campo KeyUsage de X.509 v3)

Los usos admitidos de la clave para los certificados de persona natural vienen dados por el valor de las extensiones Key Usage y Extended Key Usage de los mismos. El contenido de dichas extensiones para cada uno de los tipos de certificados de persona natural se puede consultar en el apartado 7.1.2 del presente documento.

6.2. Protección de la clave privada y controles de ingeniería de los módulos

6.2.1. Estándares para los módulos criptográficos

Las tarjetas criptográficas con certificados para firma electrónica avanzada, aptas como dispositivos seguros de creación de firma, contarán con la certificación FIPS 140-2 Nivel 2.

6.2.2. Control multipersona (k de n) de la clave privada

Las claves privadas de los certificados de persona natural no se encuentran bajo control multipersona. El control de dicha clave privada recae enteramente sobre el titular.

6.2.3. Custodia de la clave privada

La custodia de las claves privadas de los certificados de persona natural la realizan los propios titulares de estas.

6.2.4. Copia de seguridad de la clave privada

En ningún caso se realizarán copias de seguridad de las claves privadas de firma de personas naturales para garantizar el no repudio.

6.2.5. Archivo de la clave privada

Las claves privadas de firma de personas naturales nunca serán archivadas para garantizar el no repudio.

6.2.6. Transferencia de la clave privada a o desde el módulo criptográfico

En ningún caso es posible transferir las claves privadas de firma de personas naturales para garantizar el no repudio.

6.2.7. Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas de firma de personas naturales se generan en el dispositivo criptográfico en el momento de la generación de los certificados.

6.2.8. Método de activación de la clave privada

La activación de la clave privada la podrá efectuar el titular de la misma mediante el uso de su PIN.

6.2.9. Método de desactivación de la clave privada

La desactivación de la clave privada de persona natural se realizará mediante solicitud del titular del certificado electrónico. Esta desactivación se tratará como una revocación del certificado electrónico por lo que se seguirá el procedimiento establecido para tal fin.

6.2.10. Método de destrucción de la clave privada

La destrucción de la clave privada debe ser precedida por una revocación del certificado electrónico asociado a la clave, si esta estuviese todavía vigente. La DNFE dispondrá de un método de destrucción de forma que impida su robo o uso no autorizado.

6.2.11. Clasificación de los módulos criptográficos

Los módulos criptográficos utilizados cumplen el estándar FIPS 140-2 nivel 2.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave pública

Como establezca la DPC de la RPP-PKI.

6.3.2. Periodos operativos de los certificados y periodo de uso para el par de claves

El periodo de validez de los Certificados de Persona Natural es de dos (2) años desde el momento de emisión de este.

6.4. Datos de activación

6.4.1. Generación e instalación de los datos de activación

Como establezca la DPC de la RPP-PKI.

6.4.2. Protección de los datos de activación

Como establezca la DPC de la RPP-PKI.

6.4.3. Otros aspectos de los datos de activación

Como establezca la DPC de la RPP-PKI.

6.5. Controles de seguridad informática

6.5.1. Requerimientos técnicos de seguridad específicos

Como establezca la DPC de la RPP-PKI.

6.5.2. Evaluación de la seguridad informática

Como establezca la DPC de la RPP-PKI.

6.6. Controles de seguridad del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Como establezca la DPC de la RPP-PKI.

6.6.2. Controles de gestión de seguridad

Como establezca la DPC de la RPP-PKI.

6.6.3. Controles de seguridad del ciclo de vida

Como establezca la DPC de la RPP-PKI.

6.7. Controles de seguridad de la red

Como establezca la DPC de la RPP-PKI.

6.8. Sellado de tiempo

Como establezca la DPC de la RPP-PKI.

7. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

7.1. Perfil de certificado

7.1.1. Número de versión

La RPP-PKI soporta y utiliza certificados X.509 versión 3 (X.509 v3)

7.1.2. Extensiones del certificado

Las extensiones utilizadas de forma genérica en los certificados son:

- KeyUsage. Calificada como crítica.
- BasicConstraints. Calificada como crítica.
- CertificatePolicies. Calificada como no crítica.
- SubjectAlternativeName. Calificada como no crítica.
- CRLDistributionPoint. Calificada como no crítica.

A continuación, se detalla el contenido de las extensiones más significativas de los certificados de persona natural emitidos por la RPP-PKI:

7.1.2.1. Certificado de Autenticación

La estructura del certificado, referente a la extensión subject del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	PA	País
O	FIRMA ELECTRONICA	Organización
OU	PERSONA NATURAL	Unidad Organizacional
CN	[A] NOMBRE <apellidos nombre> – ID <cedula/pasaporte>	Nombre Común

Descripción del resto de campos más relevantes del perfil de certificado para el certificado de Autenticación de Persona Natural de Panamá:

Campo	Contenido Propuesto	Crítica
1. Signature Algorithm	sha256WithRSAEncryption	
2. Issuer	C=PA, O=FIRMA ELECTRONICA, CN=CA PANAMA CLASE 2	
3. Validez	2 años	
4. Subject	C=PA, O=FIRMA ELECTRONICA, OU=PERSONA NATURAL CN=[A] NOMBRE <apellidos nombre> – ID <cedula/pasaporte>	
5. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: 2048 bits	
6. Certificate Policies	Se utilizará	NO
Policy Identifier	2.16.591.1.2.2.1.1	
URL CPS	*[DPC-URL]*	
Notice Referente	Certificado sujeto a la Declaracion de Practicas de Certificacion de Firma Electronica de Panama (2012)	
7. Subject Alternate Names	Rfc822Name = Dirección de correo electrónico [OID RPP-PKI].1.1.1: Primer Nombre [OID RPP-PKI].1.1.2: Segundo Nombre [OID RPP-PKI].1.1.3: Primer Apellido [OID RPP-PKI].1.1.4: Segundo Apellido [OID RPP-PKI].1.1.5: Cédula de identidad personal [OID RPP-PKI].1.1.6: Fecha de Nacimiento	NO
8. CRLDistributionPoints	*[HTTP URI PC2 CRL]*	NO

9. Auth. Information Access	Se utilizará	NO
caIssuers	*[HTTP URI PC2 CA]*	
ocsp	*[HTTP URI OCSP]*	
10. KeyUsage	Digital Signature Key Agreement	SI
11. extKeyUsage	clientAuth (1.3.6.1.5.5.7.3.2) anyExtendedKeyUsage (2.5.29.37.0)	NO
12. Subject Key Identifier	SHA-1 hash de la clave pública	NO
13. Authority Key Identifier	Se utilizará	NO
KeyIdentifier	SHA-1 hash de la clave pública del emisor	
AuthorityCertIssuer	No utilizado	
AuthorityCertSerialNumber	No utilizado	

7.1.2.2. Certificado de Firma

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	PA	País
O	FIRMA ELECTRONICA	Organización
OU	PERSONA NATURAL	Unidad Organizacional
CN	[F] NOMBRE <apellidos nombre> – ID <cedula/pasaporte>	Nombre Común

Descripción del resto de campos más relevantes del perfil de certificado para el certificado de Firma de Persona Natural de Panamá:

Campo	Contenido Propuesto	Crítica
1. Signature Algorithm	sha256WithRSAEncryption	
2. Issuer	C=PA, O=FIRMA ELECTRONICA, CN=CA PANAMA CLASE 2	
3. Validez	2 años	
4. Subject	C=PA, O=FIRMA ELECTRONICA, OU=PERSONA NATURAL CN=[F] NOMBRE <apellidos nombre> – ID <cedula/pasaporte>	
5. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: 2048 bits	
6. Certificate Policies	Se utilizará	NO
Policy Identifier	2.16.591.1.2.2.1.2	
URL CPS	*[DPC-URL]*	
Notice Referente	Certificado sujeto a la Declaración de Prácticas de Certificación de Firma Electrónica de Panamá (2012)	
7. Subject Alternate Names	Rfc822Name = Dirección de correo electrónico [OID RPP-PKI].1.1.1: Primer Nombre [OID RPP-PKI].1.1.2: Segundo Nombre [OID RPP-PKI].1.1.3: Primer Apellido [OID RPP-PKI].1.1.4: Segundo Apellido [OID RPP-PKI].1.1.5: Cédula de identidad personal [OID RPP-PKI].1.1.6: Fecha de Nacimiento	NO
8. CRLDistributionPoints	*[HTTP URI PC2 CRL]*	NO

9. Auth. Information Access	Se utilizará	NO
caIssuers	*[HTTP URI PC2 CA]*	
ocsp	*[HTTP URI OCSP]*	
10. KeyUsage	nonRepudiation	SI
11. extKeyUsage	emailProtection (1.3.6.1.5.5.7.3.4) anyExtendedKeyUsage (2.5.29.37.0)	NO
12. Subject Key Identifier	SHA-1 hash de la clave pública	NO
13. Authority Key Identifier	Se utilizará	NO
KeyIdentifier	SHA-1 hash de la clave pública del emisor	
AuthorityCertIssuer	No utilizado	
AuthorityCertSerialNumber	No utilizado	
14. qcStatements	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)[1]	NO

7.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos: SHA256 with RSA Encryption (1.2.840.113549.1.1.11)

7.1.4. Formatos de nombres

Los certificados emitidos por la RPP-PKI contienen el distinguished name X.500 del emisor y del titular del certificado en los campos issuer name y subject name respectivamente.

7.1.5. Restricciones de los nombres

Las restricciones de los nombres se encuentran descritas en el apartado 3.1.1. del presente documento.

[1] Indica que el certificado es compatible con la definición de certificado cualificado de IETF (*RFC 3039*).

7.1.6. Identificador de objeto (OID) de la Política de Certificación

Los OID para esta PC son los siguientes:

[OID RPP-PKI].2.2.1.X.Y Política de Certificación para Certificados de Persona Natural

[OID RPP-PKI].2.2.1.1.X.Y Política de Certificación para Certificados de Autenticación de Persona Natural

[OID RPP-PKI].2.2.1.2.X.Y Política de Certificación para Certificados de Firma de Persona Natural

Dónde:

- [OID RPP-PKI] representa el OID 2.16.591.1
- X.Y representa la versión

7.1.7. Uso de la extensión "PolicyConstraints"

Como establezca la DPC de la RPP-PKI.

7.1.8. Sintaxis y semántica de los "PolicyQualifier"

El contenido de la extensión Certificate Policies puede consultarse en el apartado 7.1.2 del presente documento.

7.1.9. Tratamiento semántico para la extensión crítica "Certificate Policy"

Como establezca la DPC de la RPP-PKI.

7.2. Perfil de CRL

7.2.1. Número de versión

Como establezca la DPC de la RPP-PKI.

7.2.2. CRL y extensiones

Como establezca la DPC de la RPP-PKI.

7.3. Perfil de OCSP

7.3.1. Número(s) de versión

Como establezca la DPC de la RPP-PKI.

7.3.2. Extensiones OCSP

Como establezca la DPC de la RPP-PKI.

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1. Frecuencia o circunstancias de los controles para cada Autoridad

Como establezca la DPC de la RPP-PKI.

8.2. Identificación/cualificación del auditor

Como establezca la DPC de la RPP-PKI.

8.3. Relación entre el auditor y la Autoridad auditada

Como establezca la DPC de la RPP-PKI.

8.4. Aspectos cubiertos por los controles

Como establezca la DPC de la RPP-PKI.

8.5. Acciones a tomar como resultado de la detección de deficiencias

Como establezca la DPC de la RPP-PKI.

8.6. Comunicación de resultados

Como establezca la DPC de la RPP-PKI.

9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

9.1. Tarifas

Las tarifas correspondientes a la emisión o renovación de certificado se encuentran detalladas en la dirección https://www.firmaelectronica.gob.pa/documentos/Resolucion-JD-003-2015-Tarifas-Certificados-Electronicos.pdf

9.1.1. Tarifas de emisión o renovación de certificado

Las tarifas correspondientes a la emisión o renovación de certificado se encuentran detalladas en la dirección https://www.firmaelectronica.gob.pa/documentos/Resolucion-JD-003-2015-Tarifas-Certificados-Electronicos.pdf

9.1.2. Tarifas de acceso a los certificados

Las tarifas correspondientes a la emisión o renovación de certificado se encuentran detalladas en la dirección https://www.firmaelectronica.gob.pa/documentos/Resolucion-JD-003-2015-Tarifas-Certificados-Electronicos.pdf

9.1.3. Tarifas de acceso a la información de estado o revocación

Las tarifas correspondientes a la emisión o renovación de certificado se encuentran detalladas en la dirección https://www.firmaelectronica.gob.pa/documentos/Resolucion-JD-003-2015-Tarifas-Certificados-Electronicos.pdf

9.1.4. Tarifas de otros servicios tales como información de políticas

Las tarifas correspondientes a la emisión o renovación de certificado se encuentran detalladas en la dirección https://www.firmaelectronica.gob.pa/documentos/Resolucion-JD-003-2015-Tarifas-Certificados-Electronicos.pdf

9.1.5. Política de reembolso

Si al momento del cese de actividades por parte de la RPP-PKI, el certificado electrónico calificado de un firmante tiene una vigencia pendiente de uso superior a seis meses, la RPP-PKI deberá reembolsarle el importe de la tarifa proporcional a la vigencia no utilizada, a menos de que la RPP-PKI al cese en sus actividades haya transferido los certificados a otro prestador de servicios de certificación. (Último párrafo del art. 32 de la Ley 51 de 2008 modificada por la Ley 82 de 2012).

9.2. Responsabilidades económicas

Como establezca la DPC de la RPP-PKI.

9.3. Confidencialidad de la información

Se establece el siguiente régimen de confidencialidad de los datos relativos a la RPP-PKI:

9.3.1. Ámbito de la información confidencial

Como establezca la DPC de la RPP-PKI.

9.3.2. Información no confidencial

Como establezca la DPC de la RPP-PKI.

9.3.3. Deber de secreto profesional

Como establezca la DPC de la RPP-PKI.

9.4. Protección de la información personal

Como establezca la DPC de la RPP-PKI.

9.5. Derechos de propiedad intelectual

Como establezca la DPC de la RPP-PKI.

9.6. Representaciones y garantías

9.6.1. Obligaciones de las CA

Como establezca la DPC de la RPP-PKI.

9.6.2. Obligaciones de las RA

Como establezca la DPC de la RPP-PKI.

9.6.3. Obligaciones de los titulares de los certificados

Como establezca la DPC de la RPP-PKI.

9.6.4. Obligaciones de los terceros que confían o aceptan los certificados de RPP-PKI

Como establezca la DPC de la RPP-PKI.

9.6.5. Obligaciones de otros participantes

Como establezca la DPC de la RPP-PKI.

9.7. Exención de responsabilidades

Como establezca la DPC de la RPP-PKI.

9.8. Limitaciones de las responsabilidades

Como establezca la DPC de la RPP-PKI.

9.9. Indemnizaciones

Como establezca la DPC de la RPP-PKI.

9.10. Período de validez

9.10.1. Plazo

Esta PC entra en vigor desde el momento de su publicación en el repositorio de la RPP-PKI y se mantendrá vigente mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la Autoridad Certificadora de Panamá, momento en que obligatoriamente se dictará una nueva versión.

9.10.2. Sustitución y derogación de la PC

Esta PC será sustituida por una nueva versión con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre se aplicará en su totalidad.

Cuando la PC quede derogada se retirará del repositorio público de la RPP-PKI, si bien se conservará durante 7 años.

9.10.3. Efectos de la finalización

Las obligaciones y restricciones que establece esta PC, en referencia a auditorías, información confidencial, obligaciones y responsabilidades de la RPP-PKI, nacidas bajo su vigencia, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

9.11. Notificaciones individuales y comunicaciones con los participantes

Como establezca la DPC de la RPP-PKI.

9.12. Procedimientos de cambios en las especificaciones

9.12.1. Procedimiento para los cambios

Como establezca la DPC de la RPP-PKI.

9.12.2. Circunstancias en las que el OID debe ser cambiado

Como establezca la DPC de la RPP-PKI.

9.13. Reclamaciones

Como establezca la DPC de la RPP-PKI.

9.14. Normativa aplicable

Como establezca la DPC de la RPP-PKI.

9.15. Cumplimiento de la normativa aplicable

Como establezca la DPC de la RPP-PKI.

9.16. Estipulaciones diversas

9.16.1. Cláusula de aceptación completa

Como establezca la DPC de la RPP-PKI.

9.16.2. Independencia

En el caso de que una o más estipulaciones de esta PC sean o llegasen a ser inválidas, nulas, o inexigibles legalmente, se entenderá por no puesta, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de la PC careciera ésta de toda eficacia jurídica.

9.16.3. Resolución por la vía judicial

Como establezca la DPC de la RPP-PKI.

9.17. Otras estipulaciones

No se contemplan otras estipulaciones.